

# AFFINE EMBEDDINGS OF CANTOR SETS AND DIMENSION OF $\alpha\beta$ -SETS

DE-JUN FENG AND YING XIONG

ABSTRACT. Let  $E, F \subset \mathbb{R}^d$  be two self-similar sets, and suppose that  $F$  can be affinely embedded into  $E$ . Under the assumption that  $E$  is dust-like and has a small Hausdorff dimension, we prove the logarithmic commensurability between the contraction ratios of  $E$  and  $F$ . This gives a partial affirmative answer to Conjecture 1.2 in [9]. The proof is based on our study of the box-counting dimension of a class of multi-rotation invariant sets on the unit circle, including the  $\alpha\beta$ -sets initially studied by Engelking and Katznelson.

## 1. INTRODUCTION

For  $A, B \subset \mathbb{R}^d$ , we say that  $A$  can be *affinely embedded* into  $B$  if  $f(A) \subset B$  for some affine map  $f: \mathbb{R}^d \rightarrow \mathbb{R}^d$  of the form  $f(x) = Mx + a$ , where  $M$  is an invertible  $d \times d$  matrices and  $a \in \mathbb{R}^d$ . In this paper, we investigate the necessary conditions under which one self-similar set can be affinely embedded into another self-similar set.

Before formulating our result, we first recall some terminologies about self-similar sets. Let  $\Phi = \{\phi_i\}_{i=1}^\ell$  be an *iterated function system* (IFS) on  $\mathbb{R}^d$ , that is, a finite family of contractive mappings on  $\mathbb{R}^d$ . It is well known (cf. [15]) that there is a unique non-empty compact set  $K \subset \mathbb{R}^d$ , called the *attractor* of  $\Phi$ , such that

$$K = \bigcup_{i=1}^{\ell} \phi_i(K).$$

Correspondingly,  $\Phi$  is called a *generating IFS* of  $K$ . We say that  $\Phi$  satisfies the *open set condition* (OSC) if there exists a non-empty bounded open set  $V \subset \mathbb{R}^d$  such that  $\phi_i(V)$ ,  $1 \leq i \leq \ell$ , are pairwise disjoint subsets of  $V$ . Similarly, we say that  $\Phi$  satisfies the *strong separation condition* (SSC) if  $\phi_i(K)$  are pairwise disjoint subsets of  $K$ . The strong separation condition always implies the open set condition ([15]). When all maps in an IFS  $\Phi$  are similitudes, the attractor  $K$  of  $\Phi$  is called a *self-similar set*. By a similitude we mean a map  $\phi: \mathbb{R}^d \rightarrow \mathbb{R}^d$  of the form  $\phi(x) = \rho Px + a$ , with  $\rho > 0$ ,  $a \in \mathbb{R}^d$  and  $P$  an  $d \times d$  orthogonal matrix. A self-similar set is called *nontrivial* if it is not a singleton.

---

2000 *Mathematics Subject Classification.* 28A80, 37C45, 11B30.

*Key words and phrases.* affine embedding, Cantor sets, self-similar sets,  $\alpha\beta$ -sets.

The problem of determining whether one self-similar set can be affinely embedded into another self-similar set was first studied in [9], revealing some interesting connections to smooth embeddings and intersections of Cantors sets. It was shown [9] that, under the open set condition,<sup>1</sup> one nontrivial self-similar set  $F$  can be embedded into another self-similar set  $E$  under a  $C^1$ -diffeomorphism if and only if it can be affinely embedded into  $E$ ; moreover, if  $F$  can not be affinely embedded into  $E$ , then there is a dimension drop in the intersection of  $E$  and any  $C^1$ -image of  $F$  in the sense that

$$\dim_H(E \cap f(F)) < \min\{\dim_H E, \dim_H F\},$$

where  $f$  is any  $C^1$ -diffeomorphism on  $\mathbb{R}^d$ , and  $\dim_H$  stands for Hausdorff dimension (cf. [7, 17]).

The above affine embedding problem is also closely related to other investigations on self-similar sets and measures, including classifications of self-similar subsets of Cantor sets [10], structures of generating IFSs of Cantor sets [11, 3, 4], Hausdorff dimension of intersections of Cantor sets [5, 12], Lipschitz equivalence and Lipschitz embedding of Cantor sets [8, 2], geometric rigidity of  $\times m$ -invariant measures [13], and equidistribution from fractal measures [14].

It is natural to expect that, if one nontrivial self-similar set can be affinely embedded into another self-similar set which is totally disconnected, then the contraction ratios of these two sets should satisfy certain arithmetic relations. The following conjecture has been formulated from this view point.

**Conjecture 1.1** ([9]). *Suppose that  $E, F$  are two totally disconnected nontrivial self-similar sets in  $\mathbb{R}^d$ , generated by IFSs  $\Phi = \{\phi_i\}_{i=1}^\ell$  and  $\Psi = \{\psi_j\}_{j=1}^m$  respectively. Let  $\rho_i, \gamma_j$  denote the contraction ratios of  $\phi_i$  and  $\psi_j$ . Suppose that  $F$  can be affinely embedded into  $E$ . Then for each  $1 \leq j \leq m$ , there exist non-negative rational numbers  $t_{i,j}$  such that  $\gamma_j = \prod_{i=1}^\ell \rho_i^{t_{i,j}}$ . In particular, if  $\rho_i = \rho$  for all  $1 \leq i \leq \ell$ , then  $\log \gamma_j / \log \rho \in \mathbb{Q}$  for  $1 \leq j \leq m$ .*

We remark that the above arithmetic relations on  $\rho_i, \gamma_j$  do fulfil when  $E$  and  $F$  are dust-like (i.e.,  $\Phi$  and  $\Psi$  satisfy the SSC) and Lipschitz equivalent [8]. Nevertheless, no arithmetic conditions are needed for the Lipschitz embeddings. Indeed, it was shown in [2] that if  $E, F$  are dust-like with  $\dim_H F < \dim_H E$ , then  $F$  can be Lipschitz embedded into  $E$ .

So far Conjecture 1.1 has been considered in [9, 1, 19, 21] in the special case that  $\Phi$  is homogeneous, that is,  $\rho_i = \rho$  for all  $i$ . It was proved in [9] that the conjecture is true under the additional assumptions that  $\Phi$  is homogeneous satisfying the SSC and  $\dim_H E < 1/2$ . Recently, Algom [1] showed that in the case that  $d = 1$ , the conjecture holds under the SSC and homogeneity on  $\Phi$ , the OSC on  $\Psi$  and an additional assumption that  $\dim_H E - \dim_H F < \delta$ , where  $\delta$  is a positive constant depending

---

<sup>1</sup>Here we say that a self-similar set satisfies the open set condition if it has a generating IFS which satisfies this condition.

on  $\dim_H F$ . Very recently, Shmerkin [19] and Wu [21] independently obtained much sharper result in the case that  $d = 1$ . Shmerkin [19] proved that Conjecture 1.1 holds under the assumptions that  $d = 1$ ,  $\Phi$  is homogeneous satisfying the OSC and  $\dim_H E < 1$ . Wu [21] proved the conjecture under almost the same assumptions, except for putting the SSC on  $\Phi$  instead of the OSC.

In this paper we consider the general case that  $\Phi$  might not be homogeneous. Let  $\mathbb{Q}$  denote the set of rational numbers. For  $u_1, \dots, u_k \in \mathbb{R}$ , set

$$\text{span}_{\mathbb{Q}}(u_1, \dots, u_k) = \left\{ \sum_{i=1}^k t_i u_i : t_i \in \mathbb{Q} \right\}.$$

Then  $\text{span}_{\mathbb{Q}}(u_1, \dots, u_k)$  is a linear space over the field  $\mathbb{Q}$  with dimension  $\leq k$ .

Our main result is the following.

**Theorem 1.2.** *Under the assumptions of Conjecture 1.1, suppose in addition that  $\Phi$  satisfies the SSC and  $\dim_H E < c$ , where*

$$(1.1) \quad c = \begin{cases} 1/4, & \text{if } \ell = 2, \\ 1/4, & \text{if } \ell \geq 3, \lambda = 1, \\ 1/(2\lambda + 2), & \text{if } \ell \geq 3, \lambda > 1, \end{cases}$$

with  $\lambda = \dim \text{span}_{\mathbb{Q}}(\log \rho_1, \dots, \log \rho_\ell)$ . Then the conclusion of Conjecture 1.1 holds.

The proof of Theorem 1.2 is based on our study of the box counting dimension of certain multi-rotation invariant sets on the unit circle. To be more precise, we first introduce some notation and definitions. Let  $\mathbb{T} = \mathbb{R}/\mathbb{Z}$  denote the unit circle (which can be viewed as the unit interval  $[0, 1]$  with the endpoints being identified). Let  $\pi : \mathbb{R} \rightarrow \mathbb{T}$  be the canonical mapping defined by  $x \mapsto \{x\}$ , where  $\{x\}$  stands for the fractional part of  $x$ .

**Definition 1.3.** *Let  $\alpha_1, \dots, \alpha_\ell \in \mathbb{R}$  with  $\ell \geq 2$ . A non-empty closed set  $K \subset \mathbb{T}$  is called an  $(\alpha_1, \dots, \alpha_\ell)$ -set if*

$$K \subset \bigcup_{i=1}^{\ell} (K - \pi(\alpha_i))$$

equivalently if, whenever  $x \in K$ , then there exists  $i \in \{1, \dots, \ell\}$  so that  $x + \pi(\alpha_i) \in K$ . Moreover, a sequence  $(x_n)_{n=0}^{\infty}$  of points in  $\mathbb{T}$  is called an  $(\alpha_1, \dots, \alpha_\ell)$ -orbit if

$$x_{n+1} - x_n \in \{\pi(\alpha_1), \dots, \pi(\alpha_\ell)\}$$

for all  $n \geq 0$ .

**Definition 1.4.** *Let  $\alpha_1, \dots, \alpha_\ell \in \mathbb{R}$  with  $\ell \geq 1$ . Say that  $\alpha_1, \dots, \alpha_\ell$  are  $\mathbb{Q}_+$ -independent (mod 1) if the following equation*

$$t_1 \alpha_1 + \dots + t_\ell \alpha_\ell \equiv 0 \pmod{1}$$

in the variables  $t_1, \dots, t_\ell$  has a unique solution  $(0, \dots, 0)$  in  $\mathbb{Q}_+^\ell$ , where  $\mathbb{Q}_+$  stands for the set of non-negative rational numbers.

Similarly we can define  $\mathbb{Q}$ -independence (mod 1) via replacing  $\mathbb{Q}_+$  by  $\mathbb{Q}$  in Definition 1.4. It is clear that the  $\mathbb{Q}$ -independence (mod 1) implies the  $\mathbb{Q}_+$ -independence (mod 1).

The study of  $(\alpha_1, \dots, \alpha_\ell)$ -sets has its origin in the early works of Engelking and Katznelson [6, 16]. In 1961, Engelking [6] raised the question of existence of nowhere dense  $(\alpha, \beta)$ -sets (for short,  $\alpha\beta$ -sets), where  $\alpha, \beta$  are  $\mathbb{Q}$ -independence (mod 1). Finally in 1979, Katznelson [16] gave an affirmative answer to this question. He showed that for any such pair  $(\alpha, \beta)$ , there always exist nowhere dense  $\alpha\beta$ -sets; furthermore for certain special pairs  $(\alpha, \beta)$ , there exist  $\alpha\beta$ -sets of Hausdorff dimension 0.

In contrast to Katznelson's result, we prove the following result claiming that, any  $(\alpha_1, \dots, \alpha_\ell)$ -orbit passing through infinitely many points has a large lower box-counting dimension (cf. [7, 17] for the definition).

**Theorem 1.5.** *Let  $\alpha_1, \dots, \alpha_\ell \in \mathbb{R}$  with  $\ell \geq 2$ . Suppose that  $(x_n)_{n=0}^\infty$  is an  $(\alpha_1, \dots, \alpha_\ell)$ -orbit passing through infinitely many points. Let  $K$  be the closure of the set  $\{x_n : n \geq 0\}$ . Then the following statements hold.*

- (i) *If  $\ell = 2$ , then either  $K - K = \mathbb{T}$  or  $K$  has a non-empty interior; in particular,*

$$\underline{\dim}_B K \geq 1/2,$$

*where  $\underline{\dim}_B$  stands for lower box-counting dimension.*

- (ii) *If  $\ell \geq 2$ , then*

$$\underline{\dim}_B K \geq \begin{cases} 1, & \text{if } r = 1, \\ 1/(r+1), & \text{if } r > 1, \end{cases}$$

*where  $r = \dim_{\mathbb{Q}}(1, \alpha_1, \dots, \alpha_\ell) - 1$ .*

Notice that when  $\alpha_1, \dots, \alpha_\ell$  are  $\mathbb{Q}_+$ -independent (mod 1),  $x_n \neq x_m$  for different  $n, m$  for any  $(\alpha_1, \dots, \alpha_\ell)$ -orbit  $(x_n)_{n=0}^\infty$ . Hence by Theorem 1.5, we have the following corollary, saying that under the assumption of  $\mathbb{Q}_+$ -independence, every  $\alpha\beta$ -set or more generally, every  $(\alpha_1, \dots, \alpha_\ell)$ -set has a large lower box-counting dimension.

**Corollary 1.6.** *Let  $\alpha_1, \dots, \alpha_\ell \in \mathbb{R}$  with  $\ell \geq 2$ . Assume that  $\alpha_1, \dots, \alpha_\ell$  are  $\mathbb{Q}_+$ -independent (mod 1). Let  $K \subset \mathbb{T}$  be an  $(\alpha_1, \dots, \alpha_\ell)$ -set. Then the statements (i), (ii) listed in Theorem 1.5 hold for  $K$ .*

To our best knowledge, Theorem 1.5 seems to be new. It not only plays a key role in our proof of Theorem 1.2, but is also interesting in its own right.

This paper is organized as follows. In Section 2 we prove Theorem 1.5. In Section 3 we prove Theorem 1.2. In Section 4, we pose several questions for further study.

## 2. BOX-COUNTING DIMENSION OF MULTI-ROTATION INVARIANT SETS

In this section, we prove Theorem 1.5. Let  $\ell \in \mathbb{N}$ ,  $\ell \geq 2$  and  $\alpha_1, \dots, \alpha_\ell \in \mathbb{R}$ . Suppose that  $(x_n)_{n=0}^\infty$  is an  $(\alpha_1, \dots, \alpha_\ell)$ -orbit that takes infinitely many values. Without

loss of generality, we assume that  $x_0 = 0$ . Then by Definition 1.3, there exists a sequence  $(\omega_n)_{n=1}^\infty$  with  $\omega_n \in \{1, \dots, \ell\}$  such that

$$(2.1) \quad x_n \equiv \sum_{i=1}^n \alpha_{\omega_i} \pmod{1}, \quad n = 1, 2, \dots$$

Set  $X = \{x_n : n \geq 0\}$ . Then  $K = \overline{X}$ , where  $\overline{X}$  stands for the closure of  $X$ . Below we prove parts (i) and (ii) of Theorem 1.5 separately.

*Proof of Theorem 1.5(i).* Assume that  $\ell = 2$ . It is enough to show that either  $X - X$  is dense in  $\mathbb{T}$ , or  $\overline{X}$  has a non-empty interior. As a direct consequence,

$$2\underline{\dim}_B K = 2\underline{\dim}_B X \geq \underline{\dim}_B (X - X) = 1,$$

where the second inequality follows from the simple fact that, if  $X$  can be covered by  $k$  balls  $B_1, \dots, B_k$  of radius  $r$ , then  $X - X$  can be covered by  $B_i - B_j$  ( $1 \leq i, j \leq k$ ) and hence by  $k^2$  many balls of radius  $3r$ .

We first assume that  $\alpha_1, \alpha_2$  are  $\mathbb{Q}_+$ -dependent (mod 1). Since  $X$  contains infinitely points, one of  $\alpha_1, \alpha_2$  must be irrational. Without loss of generality, we assume that  $\alpha_2 \notin \mathbb{Q}$ . Then by the assumption of  $\mathbb{Q}_+$ -dependence (mod 1), one of the following two scenarios must occur: (a)  $\alpha_1 = \frac{p}{q} \in \mathbb{Q}$ ; (b)  $\alpha_1 \notin \mathbb{Q}$  and there exist integers  $p_1, p_2, q$  with  $p_1, q > 0$  so that  $\alpha_1 = -\frac{p_1}{q}\alpha_2 + \frac{p_2}{q}$ .

If (a) occurs, since  $X$  contains infinitely points, we have  $\omega_n = 2$  for infinitely many  $n$  and hence

$$\bigcup_{j=0}^{q-1} (X + j/q) \supset \{n\alpha_2 : n \in \mathbb{N}\} \pmod{1}.$$

Taking closure and applying the Baire category theorem, we see that  $\overline{X}$  has a non-empty interior.

If (b) occurs, since  $X$  contains infinitely points, one can check that either

$$\bigcup_{i=0}^{p_1+q-1} \bigcup_{j=0}^{q-1} \left( X + \frac{i\alpha_2 + j}{q} \right) \supset \{n\alpha_2 : n \in \mathbb{N}\} \pmod{1},$$

or

$$\bigcup_{i=0}^{p_1+q-1} \bigcup_{j=0}^{q-1} \left( X + \frac{i\alpha_2 + j}{q} \right) \supset \{-n\alpha_2 : n \in \mathbb{N}\} \pmod{1}.$$

Again by the Baire category theorem,  $\overline{X}$  has a non-empty interior.

Next assume that  $\alpha_1$  and  $\alpha_2$  are  $\mathbb{Q}_+$ -independent (mod 1). Then both of them are irrational. Below we treat the two cases separately: (c)  $\alpha_2 - \alpha_1 \in \mathbb{Q}$ , (d)  $\alpha_2 - \alpha_1 \notin \mathbb{Q}$ .

First suppose that  $\alpha_2 - \alpha_1 = p/q \in \mathbb{Q}$ . It is easy to see that for  $n \geq 1$ ,

$$x_n \equiv n\alpha_1 + p_n/q \pmod{1}$$

for some  $p_n \in \{0, 1, \dots, q-1\}$ . It follows that

$$\bigcup_{j=0}^{q-1} (X + j/q) \supset \{n\alpha_1 : n \in \mathbb{N}\} \pmod{1},$$

and so  $\overline{X}$  has a non-empty interior.

Next we consider the case that  $\alpha_2 - \alpha_1 \notin \mathbb{Q}$ . Suppose that  $X - X$  is not dense in  $\mathbb{T}$ . Then there exists  $\delta > 0$  so that  $X - X$  is not  $\delta$ -dense in  $\mathbb{T}$ .

Since  $\alpha_2 - \alpha_1 \notin \mathbb{Q}$ , there exists a positive integer  $N$  such that the set

$$\{k(\alpha_2 - \alpha_1) : k = 1, \dots, N\} \pmod{1}$$

is  $\delta$ -dense in  $\mathbb{T}$ . Write  $\tau(0) = 0$  and

$$\tau(n) = \#\{1 \leq i \leq n : \omega_i = 2\} \quad \text{for } n \geq 1,$$

where  $\#A$  stands for the cardinality of  $A$ . We claim that

$$(2.2) \quad \sup_{n, m \in \mathbb{N}} |\tau(n+m) - \tau(n) - \tau(m)| < N.$$

Suppose on the contrary that the claim is false, i.e.,

$$(2.3) \quad |\tau(n+m) - \tau(n) - \tau(m)| \geq N \quad \text{for some } n, m \in \mathbb{N}.$$

Fix such  $n, m$ . Define

$$b_j = \tau(m+j) - \tau(j), \quad j = 0, \dots, n.$$

Then  $|b_n - b_0| \geq N$  by (2.3). A direct check shows that

$$b_{j+1} - b_j = \omega_{m+j+1} - \omega_j,$$

which implies  $|b_{j+1} - b_j| \leq 1$ . Since  $|b_n - b_0| \geq N$ , we see that the set  $\{b_0, \dots, b_n\}$  contains at least  $N$  consecutive integers, say  $t+1, \dots, t+N$ . Observe that for each  $k$ ,

$$x_k \equiv (k - \tau(k))\alpha_1 + \tau(k)\alpha_2 \equiv k\alpha_1 + \tau(k)(\alpha_2 - \alpha_1) \pmod{1}.$$

Hence for  $j = 1, \dots, n$ ,

$$\begin{aligned} x_{m+j} - x_j &\equiv m\alpha_1 + (\tau(m+j) - \tau(j))(\alpha_2 - \alpha_1) \\ &\equiv m\alpha_1 + b_j(\alpha_2 - \alpha_1) \pmod{1}. \end{aligned}$$

Therefore,

$$\begin{aligned} X - X &\supset \{x_{m+j} - x_j : j = 1, \dots, n\} \\ &\equiv \{m\alpha_1 + b_j(\alpha_2 - \alpha_1) : j = 1, \dots, n\} \\ &\supset \{b' + (\alpha_2 - \alpha_1), b' + 2(\alpha_2 - \alpha_1), \dots, b' + N(\alpha_2 - \alpha_1)\} \pmod{1}, \end{aligned}$$

where  $b' = m\alpha_1 + t(\alpha_2 - \alpha_1)$ . Consequently,  $X - X$  is  $\delta$ -dense in  $\mathbb{T}$ , leading to a contraction. This proves (2.2).

Next we use (2.2) to show that  $\overline{X}$  has a non-empty interior. Indeed by (2.2), we have

$$\tau(n+m) + N \leq (\tau(n) + N) + (\tau(m) + N)$$

and

$$N - \tau(n+m) \leq (N - \tau(n)) + (N - \tau(m)),$$

that is, the two sequences  $(\tau(n) + N)_{n \geq 1}$  and  $(N - \tau(n))_{n \geq 1}$  are both subadditive. It follows that the limit  $\tau = \lim_{n \rightarrow \infty} \tau(n)/n$  exists, and moreover,

$$\tau = \inf_{n \geq 1} \frac{\tau(n) + N}{n}, \quad -\tau = \inf_{n \geq 1} \frac{N - \tau(n)}{n}.$$

That means  $|\tau(n) - n\tau| \leq N$  for all  $n \geq 1$ , and so

$$(2.4) \quad |\tau(n) - [n\tau]| \leq N \quad \text{for all } n \geq 1.$$

Set  $\tau' = (1 - \tau)\alpha_1 + \tau\alpha_2$ , and let

$$y_n = \{n\tau'\} - \{n\tau\}(\alpha_2 - \alpha_1) \pmod{1} \quad \text{for } n \geq 1.$$

Then

$$\begin{aligned} y_n &\equiv n((1 - \tau)\alpha_1 + \tau\alpha_2) - \{n\tau\}(\alpha_2 - \alpha_1) \\ &\equiv n\alpha_1 + [n\tau](\alpha_2 - \alpha_1) \\ &\equiv n\alpha_1 + \tau(n)(\alpha_2 - \alpha_1) + z_n \\ &\equiv x_n + z_n \pmod{1}, \end{aligned}$$

where  $z_n := ([n\tau] - \tau(n))(\alpha_2 - \alpha_1)$ . By (2.4), for all  $n \geq 1$ ,

$$z_n \in \{k(\alpha_2 - \alpha_1) : k \in \mathbb{Z} \text{ and } |k| \leq N\} =: Z.$$

Let  $Y = \{y_n : n \in \mathbb{N}\}$ ; then  $Y \subset X + Z \pmod{1}$ . Since  $Z$  is finite, by Baire category theorem,  $\overline{X}$  has a non-empty interior if so does  $\overline{Y}$ .

It remains to show that  $\overline{Y}$  has a non-empty interior. Since  $\tau \in [0, 1]$ ,  $\tau$  and  $\tau'$  can not be rational numbers simultaneously (otherwise,  $\alpha_1$  and  $\alpha_2$  are not  $\mathbb{Q}_+$ -independent  $\pmod{1}$ ). Therefore,

$$W := \overline{\{(\{n\tau\}, \{n\tau'\}) : n \geq 1\}}$$

is an infinite compact subgroup of  $\mathbb{T}^2 = \mathbb{R}^2/\mathbb{Z}^2$ . It is either the whole group  $\mathbb{T}^2$  or finitely many lines in  $\mathbb{T}^2$  with rational slope. Notice that

$$\overline{Y} = \overline{\{\{n\tau'\} - \{n\tau\}(\alpha_2 - \alpha_1) \pmod{1} : n \geq 1\}},$$

which can be regarded as the image of  $W$  under certain projection along an *irrational* direction since  $\alpha_2 - \alpha_1 \notin \mathbb{Q}$ . Consequently,  $\overline{Y}$  has a non-empty interior and so does  $\overline{X}$ . This completes the proof of Theorem 1.5(i).  $\square$

Before proving Theorem 1.5(ii), we first give two simple lemmas.

**Lemma 2.1.** *Consider the following system of linear equations in the variables  $z_1, \dots, z_\ell$ :*

$$(2.5) \quad \sum_{i=1}^{\ell} a_{i,j} z_i = b_j, \quad j = 1, 2, \dots,$$

where  $a_{i,j}, b_j \in \mathbb{Q}$  for all  $i, j$ . Suppose that the system has a real solution. Then it must have a rational solution.

*Proof.* This is a classical result in linear algebra.  $\square$

**Lemma 2.2.** *For  $A \subset \mathbb{T}$  and  $\delta > 0$ , let  $N_\delta(A)$  denote the smallest number of intervals of length  $\delta$  that are needed to cover  $A$ . Then for any positive integer  $p$ , we have*

$$N_{p\delta}(pA(\bmod 1)) \leq N_\delta(A).$$

*Proof.* Suppose that  $A$  can be covered by intervals  $I_1, \dots, I_k$ . Then  $pA(\bmod 1)$  can be covered by the intervals  $pI_1(\bmod 1), \dots, pI_k(\bmod 1)$ .  $\square$

*Proof of Theorem 1.5(ii).* First observe that  $\dim \text{span}_{\mathbb{Q}}(1, \alpha_1, \dots, \alpha_\ell) =: 1 + r > 1$ , otherwise  $\alpha_1, \dots, \alpha_\ell$  are all rationals and hence  $X$  is a finite set, which leads to a contradiction. Therefore,  $r \geq 1$ . Pick a suitable basis  $1, \beta_1, \dots, \beta_r$  of  $\text{span}_{\mathbb{Q}}(1, \alpha_1, \dots, \alpha_\ell)$  so that

$$(2.6) \quad \alpha_i = \sum_{j=1}^r p_{i,j} \beta_j + q_i, \quad i = 1, \dots, \ell,$$

for some  $p_{i,j} \in \mathbb{Z}$  and  $q_i \in \mathbb{Q}$ .

For  $i = 1, \dots, \ell$ , set

$$N_i(0) = 0, \text{ and } N_i(n) = \#\{1 \leq j \leq n : \omega_j = i\} \quad \text{for } n \geq 1.$$

Write

$$b_j(n) = \sum_{i=1}^{\ell} p_{i,j} N_i(n), \quad 1 \leq j \leq r, \quad n \geq 0.$$

Then  $b_j(n) \in \mathbb{Z}$ , and moreover,

$$(2.7) \quad b_j(n+1) - b_j(n) = \sum_{i=1}^{\ell} p_{i,j} (N_i(n+1) - N_i(n)) = p_{\omega_{n+1}, j}.$$

Clearly, we have

$$(2.8) \quad \begin{aligned} x_n &\equiv \sum_{i=1}^{\ell} N_i(n) \alpha_i \\ &\equiv \sum_{i=1}^{\ell} \left( \left( \sum_{j=1}^r p_{i,j} N_i(n) \beta_j \right) + q_i N_i(n) \right) \\ &\equiv \sum_{j=1}^r b_j(n) \beta_j + \sum_{i=1}^{\ell} q_i N_i(n) \pmod{1}. \end{aligned}$$



As  $q_i \in \mathbb{Q}$ , the term  $c_n := \sum_{i=1}^{\ell} q_i N_i(n) \pmod{1}$  can take only finitely many different values. However, by assumption,  $x_n$  can take infinitely many different values, thus the sequence  $(b_1(n), \dots, b_r(n))_{n \geq 0}$  of integer vectors is unbounded. Therefore, there exist  $r_0 \in \{1, \dots, r\}$  and a strictly increasing sequence  $(n_s)_{s \geq 1}$  of positive integers such that

$$(2.9) \quad |b_{r_0}(n_s)| = \max_{1 \leq j \leq r} |b_j(n_s)| \text{ for all } s \geq 1, \text{ and } \lim_{s \rightarrow \infty} |b_{r_0}(n_s)| = \infty.$$

Choose a positive integer  $M$  so that  $M > 1 + \sum_{j=1}^r |\beta_j|$ . Then define  $\beta_1^*, \dots, \beta_r^*$  by

$$\beta_j^* = \begin{cases} \beta_j & \text{if } j \in \{1, \dots, r\} \setminus \{r_0\}, \\ \beta_{r_0} + M & \text{if } j = r_0. \end{cases}$$

Correspondingly, set  $q_i^* = q_i - M p_{i,r_0}$  for  $1 \leq i \leq \ell$ . Clearly  $\{1, \beta_1^*, \dots, \beta_r^*\}$  is still a basis of  $\text{span}_{\mathbb{Q}}(1, \alpha_1, \dots, \alpha_{\ell})$  and it satisfies the following relations:

$$(2.10) \quad \alpha_i = \sum_{j=1}^r p_{i,j} \beta_j^* + q_i^*, \quad i = 1, \dots, \ell.$$

Similar to (2.8), for  $n \geq 0$  we have

$$(2.11) \quad x_n \equiv \sum_{j=1}^r b_j(n) \beta_j^* + \sum_{i=1}^{\ell} q_i^* N_i(n) \pmod{1}$$

Set

$$(2.12) \quad B(n) = \sum_{j=1}^r b_j(n) \beta_j^* = \sum_{j=1}^r \sum_{i=1}^{\ell} p_{i,j} N_i(n) \beta_j^*.$$

Then by (2.9), we have

$$\begin{aligned} |B(n_s)| &= \left| \sum_{j=1}^r b_j(n_s) \beta_j^* \right| \\ &\geq |b_{r_0}(n_s)| \cdot \left( M - \sum_{j=1}^r |\beta_j| \right) \\ &\geq |b_{r_0}(n_s)|. \end{aligned}$$

Hence, by (2.9) again, we see that

$$(2.13) \quad \lim_{s \rightarrow \infty} |B(n_s)| = \infty,$$

and the sequence

$$(2.14) \quad \left( \frac{b_1(n_s)}{B(n_s)}, \dots, \frac{b_r(n_s)}{B(n_s)} \right)_{s \geq 1} \text{ is bounded.}$$

Now we define a new sequence  $(\tilde{x}_n)_{n \geq 0}$  of points in  $\mathbb{T}$  so that  $\tilde{x}_0 = 0$  and

$$(2.15) \quad \tilde{x}_n \equiv B(n) \pmod{1} \quad \text{for } n \geq 1.$$

By (2.11) and (2.12), we see that

$$(2.16) \quad x_n - \tilde{x}_n \equiv \sum_{i=1}^{\ell} q_i^* N_i(n) \pmod{1},$$

which can only take finitely many different values.

Next we prove a key lemma about the distribution of the sequence  $(\tilde{x}_n)$ .

**Lemma 2.3.** *There exists  $k_0 \in \mathbb{N}$  such that*

$$\sup_{n \geq 1} \|k\tilde{x}_n\| \geq 1/5$$

for all integers  $k \geq k_0$ , where  $\|x\| = \inf\{|x - z| : z \in \mathbb{Z}\}$ .

*Proof.* We prove the lemma by contradiction. Suppose that the lemma is false. Then there exists a strictly increasing sequence  $(k_l)_{l \geq 1}$  of positive integers so that

$$(2.17) \quad \|k_l \tilde{x}_n\| < 1/5 \quad \text{for all } n, l \geq 1.$$

Let  $\{x\}$  and  $[x]$  denote the fractional part and integer part of the real number  $x$ , respectively.

Since the sequence  $(\sum_{j=1}^r p_{i,j} \{k_l \beta_j^*\})_{l \geq 1}$  is bounded for every  $i \in \{1, \dots, \ell\}$ , by taking a subsequence of  $(k_l)_{l \geq 1}$  if necessary, we can assume that

$$(2.18) \quad \left| \sum_{j=1}^r p_{i,j} (\{k_l \beta_j^*\} - \{k_m \beta_j^*\}) \right| < 1/5 \quad \text{for } 1 \leq i \leq \ell \text{ and } l, m \geq 1.$$

For each  $l \geq 1$ , define  $y_{l,0} = 0$  and

$$(2.19) \quad y_{l,n} = \sum_{j=1}^r b_j(n) \{k_l \beta_j\} = \sum_{j=1}^r \sum_{i=1}^{\ell} p_{i,j} N_i(n) \{k_l \beta_j\} \quad \text{for } n \geq 1.$$

By (2.15) and (2.12), we have  $y_{l,n} \equiv k_l \tilde{x}_n \pmod{1}$ , and so  $\|y_{l,n}\| < 1/5$  by (2.17). We claim that

$$(2.20) \quad |y_{l,n} - y_{m,n}| < 2/5 \quad \text{for all } l, m \in \mathbb{N} \text{ and } n \geq 0.$$

To see it, we proceed by induction on  $n$ . Clearly (2.20) holds for  $n = 0$ , since by definition  $y_{l,0} = 0$  for all  $l \geq 1$ . Now suppose that  $|y_{l,n} - y_{m,n}| < 2/5$  for all  $l, m \in \mathbb{N}$  and some  $n \geq 0$ . Since  $\|y_{l,n}\| < 1/5$  and  $\|y_{m,n}\| < 1/5$ , by (2.20) there exists  $z \in \mathbb{Z}$  such that

$$(2.21) \quad y_{l,n}, y_{m,n} \in (z - 1/5, z + 1/5).$$

Observe that

$$\begin{aligned}
 & |(y_{l,n+1} - y_{l,n}) - (y_{m,n+1} - y_{m,n})| \\
 &= \left| \sum_{j=1}^r (b_j(n+1) - b_j(n)) (\{k_l\beta_j^*\} - \{k_m\beta_j^*\}) \right| \quad (\text{by (2.19)}) \\
 (2.22) \quad &= \left| \sum_{j=1}^r p_{\omega_{n+1},j} (\{k_l\beta_j^*\} - \{k_m\beta_j^*\}) \right| \quad (\text{by (2.7)}) \\
 &\leq 1/5 \quad (\text{by (2.18)}).
 \end{aligned}$$

Since  $\|y_{l,n+1}\| < 1/5$ , we have  $|y_{l,n+1} - z'| < 1/5$  for some  $z' \in \mathbb{Z}$ , and so by (2.21),

$$|y_{l,n+1} - y_{l,n} - (z' - z)| < 2/5.$$

Combining the above inequality with (2.22) yields that

$$|y_{m,n+1} - y_{m,n} - (z' - z)| < 3/5.$$

Thus, by (2.21),  $|y_{m,n+1} - z'| < 4/5$ . Combining this with  $\|y_{m,n+1}\| < 1/5$ , we have  $|y_{m,n+1} - z'| < 1/5$ . Consequently,  $|y_{l,n+1} - y_{m,n+1}| < 2/5$ . This completes the proof of (2.20).

By (2.19) and (2.20),

$$\left| \sum_{j=1}^r b_j(n) (\{k_l\beta_j^*\} - \{k_m\beta_j^*\}) \right| < \frac{2}{5}.$$

That is

$$\left| (k_l - k_m)B(n) - \sum_{j=1}^r b_j(n) ([k_l\beta_j^*] - [k_m\beta_j^*]) \right| < \frac{2}{5}.$$

Replacing  $n$  by  $n_s$  and dividing both sides by  $|(k_l - k_m)B(n_s)|$  gives

$$(2.23) \quad \left| \sum_{j=1}^r \frac{b_j(n_s)}{B(n_s)} \cdot \frac{[k_l\beta_j^*] - [k_m\beta_j^*]}{k_l - k_m} - 1 \right| < \frac{2}{5|(k_l - k_m)B(n_s)|}.$$

By (2.14), the sequence

$$\left( \frac{b_1(n_s)}{B(n_s)}, \dots, \frac{b_r(n_s)}{B(n_s)} \right)_{s \geq 1}$$

is bounded and hence has an accumulation point, say  $(t_1, \dots, t_r)$ . By (2.13) and (2.23), we have

$$\sum_{j=1}^r t_j \frac{[k_l\beta_j^*] - [k_m\beta_j^*]}{k_l - k_m} = 1 \quad \text{for all distinct } l, m \in \mathbb{N}.$$

Since  $\frac{[k_l\beta_j^*] - [k_m\beta_j^*]}{k_l - k_m} \in \mathbb{Q}$ , by Lemma 2.1, there exist  $u_1, \dots, u_r \in \mathbb{Q}$  such that

$$\sum_{j=1}^r u_j \frac{[k_l\beta_j^*] - [k_m\beta_j^*]}{k_l - k_m} = 1 \quad \text{for all distinct } l, m \in \mathbb{N}.$$

Finally, letting  $k_l - k_m \rightarrow \infty$ , we have  $\sum_{j=1}^r u_j \beta_j^* = 1$ , which contradicts the fact that  $1, \beta_1^*, \dots, \beta_r^*$  are  $\mathbb{Q}$ -independent. This completes the proof of the lemma.  $\square$

Let us continue the proof of Theorem 1.5(ii). We consider the cases  $r = 1$  and  $r > 1$  separately.

First assume that  $r = 1$ . In this case, we show that  $K$  has non-empty interior. For convenience, write  $\beta = \beta_1^*$  and  $p_i := p_{i,1}$ . Then  $\beta$  is irrational and

$$(2.24) \quad \alpha_i = p_i \beta + q_i^* \quad \text{for } i = 1, \dots, \ell.$$

Recall that  $p_i \in \mathbb{Z}$  and  $q_i^* \in \mathbb{Q}$ . Pick  $q \in \mathbb{N}$  such that all  $q_i^*$  are the integral multiples of  $1/q$ . Let  $p = \max_{1 \leq i \leq \ell} |p_i|$ . Since the set  $X = \{x_n : n \geq 1\}$  is infinite, we have  $p \geq 1$  and moreover, by the expression (2.24) of  $\alpha_i$ , it is not hard to see that

$$\begin{aligned} & \text{either } \bigcup_{i=-p}^p \bigcup_{j=-q}^q \left( X + i\beta + \frac{j}{q} \right) \supset \{n\beta : n \in \mathbb{N}\} \pmod{1} \\ & \text{or } \bigcup_{i=-p}^p \bigcup_{j=-q}^q \left( X + i\beta + \frac{j}{q} \right) \supset \{-n\beta : n \in \mathbb{N}\} \pmod{1}. \end{aligned}$$

Taking closure and applying the Baire category theorem, we see that  $K = \overline{X}$  has a non-empty interior.

Next assume  $r \geq 2$ . Let  $m = \max_{1 \leq i \leq \ell} \sum_{j=1}^r |p_{i,j}|$ . We claim that for every  $n \in \mathbb{N}$ , there exists  $k_n \in \{1, \dots, (mn)^r + 1\}$  such that

$$(2.25) \quad \|k_n \beta_j^*\| \leq \frac{1}{mn}, \quad j = 1, \dots, r.$$

To prove this claim, fix  $n \in \mathbb{N}$  and partition the unit cube  $[0, 1]^r$  into  $(mn)^r$  sub-cubes of side length  $\frac{1}{mn}$ . Consider the following  $(mn)^r + 1$  vectors

$$v_k = (k\beta_1^*, \dots, k\beta_r^*) \pmod{1}, \quad k = 1, \dots, (mn)^r + 1.$$

By the pigeonhole principle, two of them, say  $v_k$  and  $v_{k'}$ , are contained in the same subcube, and thus  $v_k - v_{k'} \in [-\frac{1}{mn}, \frac{1}{mn}]^r$ . Then we have  $\|(k' - k)\beta_j^*\| \leq \frac{1}{mn}$  for all  $j \in \{1, \dots, r\}$ . The claim is proved by taking  $k_n = |k' - k|$ .

Pick  $q \in \mathbb{N}$  such that all  $q_i^*$  are the integral multiples of  $1/q$ . By (2.10) and (2.25), we have

$$(2.26) \quad \|k_n q \alpha_i\| \leq \sum_{j=1}^r (q |p_{i,j}| \cdot \|k_n \beta_j^*\|) \leq qm \cdot \frac{1}{mn} = \frac{q}{n}, \quad i = 1, \dots, \ell, \quad n \geq 1.$$

Define  $y_{n,s} \in \mathbb{T}$  so that

$$(2.27) \quad y_{n,s} \equiv k_n q x_s \pmod{1}, \quad n \geq 1, \quad s = 0, 1, \dots,$$

and let  $Y_n = \{y_{n,s} : s = 0, 1, \dots\} \subset \mathbb{T}$ . By (2.26) and the definition of  $x_s$ , we have  $\|y_{n,s+1} - y_{n,s}\| \leq q/n$  for each  $s \geq 0$ . It follows that

$$I_n := \bigcup_{s \geq 0} \left[ y_{n,s} - \frac{q}{2n}, y_{n,s} + \frac{q}{2n} \right] \pmod{1}$$

is an interval in  $\mathbb{T}$  containing  $y_{n,0} = 0$ .

By (2.16), we have  $qx_n = q\tilde{x}_n \pmod{1}$  for each  $n \geq 1$ . Therefore, by Lemma 2.3, there exists  $k_0 > 0$  such that

$$a := \inf_{k \geq k_0} \sup_{s \geq 0} \|kqx_s\| = \inf_{k \geq k_0} \sup_{s \geq 0} \|kq\tilde{x}_s\| \geq \frac{1}{5}.$$

Hence by (2.27), for any  $n$  so that  $k_n > k_0$ , we have  $\sup_{s \geq 0} \|y_{n,s}\| \geq a > 0$ , and hence the length of  $I_n$  is not less than  $a$ . It follows that

$$N_{q/n}(Y_n) \geq an/q,$$

where  $N_\delta(A)$  stands for the smallest number of intervals of length  $\delta$  that are needed to cover  $A$ . Since  $Y_n = k_n qX \pmod{1}$ , by Lemma 2.2, we have

$$N_{1/(nk_n)}(X) \geq N_{q/n}(Y_n) \geq an/q.$$

Since  $k_n \leq (mn)^r + 1$ , we have

$$N_{1/(2m^r n^{r+1})}(X) \geq N_{q/n}(X) \geq an/q.$$

Noticing that the above inequality holds for all  $n \in \mathbb{N}$  and  $m, q, r$  are constant, we have

$$\underline{\dim}_B X \geq \liminf_{n \rightarrow \infty} \frac{\log(an/q)}{\log(2m^r n^{r+1})} = \frac{1}{r+1}.$$

Thus we have  $\underline{\dim}_B K = \underline{\dim}_B X \geq 1/(r+1)$ .  $\square$

### 3. THE PROOF OF THEOREM 1.2

We begin with a lemma about orthogonal groups. Let  $\mathcal{O}(d)$  be the group of  $d \times d$  orthogonal matrices operated by matrix multiplication.

**Lemma 3.1.** *For every  $P \in \mathcal{O}(d)$ , there exists  $k \in \mathbb{N}$  such that the closure of  $\{P^{kj} : j \geq 0\}$  in  $\mathcal{O}(d)$  is a connected subgroup of  $\mathcal{O}(d)$ .*

*Proof.* This result might be well known, however we are not able to find a reference, so a proof is included for the reader's convenience.

Let  $P \in \mathcal{O}(d)$ , and let  $W$  be the closure of  $\{P^j : j \geq 0\}$  in  $\mathcal{O}(d)$ . It is not hard to see that  $W$  is a compact Abelian subgroup of  $\mathcal{O}(d)$ . Hence by the Cartan theorem (cf. [18, Theorem 3.3.1]),  $W$  is also a Lie group. Let  $W_0$  be the connected component of  $W$  containing the unit element  $I$ . Then  $W_0$  is a closed normal subgroup of  $W$ , and it is also open in  $W$  (cf. [18, Lemma 2.1.4]). By the finite covering theorem,  $W$  has only finitely many connected branches. It follows that the quotient group  $W/W_0$  is finite.

Let  $\mathbb{Z}_0 = \{j \in \mathbb{Z} : P^j \in W_0\}$ . Then  $\mathbb{Z}_0$  is a subgroup of  $\mathbb{Z}$ . Since  $W/W_0$  is finite, there are distinct  $j_1, j_2 \in \mathbb{Z}$  such that  $P^{j_1}$  and  $P^{j_2}$  both belong to a coset of  $W_0$ . Hence  $P^{j_2-j_1} \in W_0$ , and consequently,  $\mathbb{Z}_0$  contains a nonzero element  $j_2 - j_1$ . Therefore,  $\mathbb{Z}_0 = k\mathbb{Z}$  for some  $k \geq 1$ . We claim that  $W_0$  is the closure of  $\{P^{kj} : j \geq 0\}$ , from which the lemma follows since  $W_0$  is connected.

Clearly  $W_0$  contains the closure of  $\{P^{kj} : j \geq 0\}$ . Conversely, since  $W_0$  is open and disjoint from  $\{P^j : k \nmid j\}$ , it is also disjoint from the closure of  $\{P^j : k \nmid j\}$ . Thus,  $W_0$  is contained in the closure of  $\{P^{kj} : j \geq 0\}$ . This completes the proof of the lemma.  $\square$

*Proof of Theorem 1.2.* For brevity, we write  $\phi_I = \phi_{i_1} \circ \cdots \circ \phi_{i_n}$  and  $\rho_I = \rho_{i_1} \cdots \rho_{i_n}$  for  $I = i_1 \dots i_n \in \{1, \dots, \ell\}^n$ . Similarly, we also use the abbreviations  $\psi_J$  and  $\gamma_J$  for  $J \in \{1, \dots, m\}^n$ .

Since  $F$  can be affinely embedded into  $E$ , there exist an invertible real  $d \times d$  matrix  $M$  and  $b \in \mathbb{R}^d$  such that

$$(3.1) \quad M(F) + b \subset E.$$

Without loss of generality, we only prove that the conclusion of Theorem 1.2 holds for  $j = 1$ , that is, there exist non-negative rational numbers  $t_{1,i}$ ,  $i = 1, \dots, \ell$ , such that

$$\gamma_1 = \prod_{i=1}^{\ell} \rho_i^{t_{1,i}}.$$

This is equivalent to show that  $\alpha_1, \dots, \alpha_\ell$  are not  $\mathbb{Q}_+$ -independent (mod 1), where

$$\alpha_i := -\frac{\log \rho_i}{\log \gamma_1} \quad \text{for } i \in \{1, \dots, \ell\}.$$

Let  $P_1$  be the orthogonal part of  $\psi_1$ . By Lemma 3.1, there exists  $l \in \mathbb{N}$  such that the closure of  $\{P_1^{lj} : j \geq 0\}$  in  $\mathcal{O}(d)$  is a connected subgroup of  $\mathcal{O}(d)$ . In what follows, replacing  $\psi_1$  by  $\psi_1^l$  if necessary, we may always assume that the closure  $\{P_1^j : j \geq 0\}$  in  $\mathcal{O}(d)$  is connected.

Let  $x$  be the fixed point of  $\psi_1$ . Then  $x \in \psi_1^n(F)$  for any integer  $n \geq 0$ . By (3.1), we have

$$y := M(x) + b \in E,$$

and thus there exists a symbolic coding  $i_1 i_2 \cdots \in \{1, \dots, \ell\}^{\mathbb{N}}$  such that

$$(3.2) \quad y = \lim_{n \rightarrow \infty} \phi_{i_1 \dots i_n}(0).$$

Clearly  $y \in \phi_{i_1 \dots i_n}(E)$  for each  $n \geq 0$ , which implies that

$$(3.3) \quad (M(\psi_1^k(F)) + b) \cap \phi_{i_1 \dots i_n}(E) \neq \emptyset \quad \text{for any } k, n \geq 0.$$

Since  $\Phi$  satisfies the strong separation condition, we have

$$(3.4) \quad \delta := \min_{i \neq j} \text{dist}(\phi_i(E), \phi_j(E)) > 0.$$

Moreover, for each  $n \in \mathbb{N}$ , we have

$$(3.5) \quad \text{dist}(\phi_{i_1 \dots i_n}(E), E \setminus \phi_{i_1 \dots i_n}(E)) \geq \rho_{i_1 \dots i_{n-1}} \delta > 0.$$

For  $k, n \geq 0$ , by (3.3) and (3.5) we have

$$(3.6) \quad M(\psi_1^k(F)) + b \subset \phi_{i_1 \dots i_n}(E) \quad \text{if} \quad \text{diam}(M(\psi_1^k(F))) < \rho_{i_1 \dots i_{n-1}} \delta.$$

Now for  $n \geq 1$ , define

$$(3.7) \quad s_n = \min\{k \geq 0: M(\psi_1^k(F)) + b \subset \phi_{i_1 \dots i_n}(E)\}.$$

Then by (3.6),  $s_n < \infty$ . Write

$$(3.8) \quad \begin{aligned} \|M\| &= \max\{|Mv|: v \in \mathbb{R}^d \text{ with } |v| = 1\}, \\ \|M\| &= \min\{|Mv|: v \in \mathbb{R}^d \text{ with } |v| = 1\}, \end{aligned}$$

where  $|\cdot|$  denotes the standard Euclidean norm.

By (3.7)-(3.8), we have

$$\|M\| \gamma_1^{s_n} \text{diam } F \leq \text{diam } M(\psi_1^{s_n}(F)) \leq \text{diam } \phi_{i_1 \dots i_n}(E) = \rho_{i_1 \dots i_n} \text{diam } E.$$

Thus, we have

$$(3.9) \quad \frac{\gamma_1^{s_n}}{\rho_{i_1 \dots i_n}} \leq \frac{\text{diam } E}{\|M\| \text{diam } F} \quad \text{for all } n \geq 1.$$

For the lower bound, we claim that

$$(3.10) \quad \frac{\gamma_1^{s_n}}{\rho_{i_1 \dots i_n}} \geq \frac{\gamma_1 \delta}{\rho^* \|M\| \text{diam } F} \quad \text{if } s_n \geq 1,$$

where  $\delta$  is defined as in (3.4) and  $\rho^* := \max_{1 \leq i \leq \ell} \rho_i$ . Indeed, suppose that (3.10) fails for some  $n$  with  $s_n \geq 1$ . Then

$$\text{diam } M(\psi_1^{s_n-1}(F)) \leq \|M\| \gamma_1^{s_n-1} \text{diam } F < (\rho^*)^{-1} \rho_{i_1 \dots i_n} \delta \leq \rho_{i_1 \dots i_{n-1}} \delta.$$

By (3.6),  $M(\psi_1^{s_n-1}(F)) + b \subset \phi_{i_1 \dots i_n}(E)$ , which contradicts the definition of  $s_n$ . This completes the proof of (3.10).

For  $1 \leq i \leq \ell$ , let  $O_i$  be the orthogonal part of  $\phi_i$ . From  $M(\psi_1^{s_n}(F)) + b \subset \phi_{i_1 \dots i_n}(E)$  we have

$$(\phi_{i_1 \dots i_n})^{-1}(M(\psi_1^{s_n}(F)) + b) \subset E.$$

Hence

$$\rho_{i_1 \dots i_n}^{-1} \gamma_1^{s_n} Q_n(F) + b_n \subset E$$

for some  $b_n \in \mathbb{R}^d$ , where  $Q_n = (O_{i_1} \circ \dots \circ O_{i_n})^{-1} M P_1^{s_n}$ . Taking algebraic difference, we have

$$(3.11) \quad \rho_{i_1 \dots i_n}^{-1} \gamma_1^{s_n} Q_n(F - F) \subset E - E, \quad n \geq 1.$$

Fix a nonzero vector  $v \in F - F$ . For any integer  $k \geq 0$ , we have

$$\gamma_1^k P_1^k v \in \psi_1^k(F) - \psi_1^k(F) \subset F - F.$$

Hence by (3.11),

$$\rho_{i_1 \dots i_n}^{-1} \gamma_1^{s_n+k} Q_n(P_1^k v) \in E - E, \quad \forall n \geq 1, k \geq 0.$$

Taking norm on both sides yields

$$(3.12) \quad \rho_{i_1 \dots i_n}^{-1} \gamma_1^{s_n+k} |MP_1^{s_n+k} v| \in \{|x_1 - x_2| : x_1, x_2 \in E\}, \quad \forall n \geq 1, k \geq 0.$$

Next we continue our arguments according to whether the sequence  $(|MP_1^j v|)_{j=0}^\infty$  is constant.

*Case (i):* the sequence  $(|MP_1^j v|)_{j=0}^\infty$  is constant.

In this case, applying (3.12) with  $k = 0$  we obtain

$$U := \{|x_1 - x_2| : x_1, x_2 \in E\} \supset V := \{\rho_{i_1 \dots i_n}^{-1} \gamma_1^{s_n} a : n \geq 1\},$$

where  $a$  is the positive constant  $|MP_1^j v|$ . Set  $b_* = \inf V$  and  $b^* = \sup V$ . By (3.9)-(3.10),  $0 < b_* < b^* < \infty$ .

Define  $f : [b_*, b^*] \rightarrow \mathbb{T}$  by  $f(t) = \log t / \log \gamma_1 \pmod{1}$ . Notice that  $[b_*, b^*]$  can be written as the union of finitely many disjoint subintervals of the form  $[b_*, b^*] \cap [\gamma_1^{n+1}, \gamma_1^n]$  with  $n \in \mathbb{Z}$ , and restricted on each non-empty interval  $[b_*, b^*] \cap [\gamma_1^{n+1}, \gamma_1^n]$ ,  $f$  is Lipschitz. Hence we have

$$(3.13) \quad \overline{\dim}_B f(V) \leq \overline{\dim}_B V \leq \overline{\dim}_B U \leq \overline{\dim}_B (E - E) \leq \overline{\dim}_B E \times E = 2 \dim_H E.$$

where  $\overline{\dim}_B$  stands for upper box-counting dimension (cf. [7]). Recall that  $\alpha_i = -\log \rho_i / \log \gamma_1$  for  $1 \leq i \leq \ell$ . Clearly,

$$(3.14) \quad \dim \text{span}_{\mathbb{Q}}(\alpha_1, \dots, \alpha_\ell) = \dim \text{span}_{\mathbb{Q}}(\log \rho_1, \dots, \log \rho_\ell) =: \lambda.$$

Let  $\omega = i_1 i_2 \dots \in \{1, \dots, \ell\}^\mathbb{N}$ , where  $i_1 i_2 \dots$  is the symbolic coding of  $y$  (see (3.2)). Define a sequence  $(x_n(\omega))_{n=1}^\infty \subset \mathbb{T}$  so that

$$x_n(\omega) \equiv \sum_{k=1}^n \alpha_{i_k} \pmod{1} \quad \text{for } n \geq 1.$$

Set  $X(\omega) = \{x_n(\omega) : n \in \mathbb{N}\}$ . Then we have

$$f(V) \supset X(\omega) + \frac{\log a}{\log \gamma_1} \pmod{1}.$$

Combining this with (3.13) yields

$$(3.15) \quad \dim_H E \geq (1/2) \overline{\dim}_B X(\omega).$$

Now suppose on the contrary that  $\alpha_1, \dots, \alpha_\ell$  are  $\mathbb{Q}_+$ -independent  $\pmod{1}$ . Notice that  $\overline{X(\omega)}$  is an  $(\alpha_1, \dots, \alpha_\ell)$ -set. By Corollary 1.6, we have

$$\overline{\dim}_B \overline{X(\omega)} \geq \begin{cases} 1/2, & \text{if } \ell = 2, \\ 1, & \text{if } \ell \geq 3, r = 1, \\ 1/(r+1), & \text{if } \ell \geq 3, r > 1, \end{cases}$$

where  $r = \dim \text{span}_{\mathbb{Q}}(1, \alpha_1, \dots, \alpha_\ell) - 1$ . By (3.14),  $\lambda = \dim \text{span}_{\mathbb{Q}}(\alpha_1, \dots, \alpha_\ell) \geq r$ .



Hence by (3.15), we have

$$\dim_H E \geq \frac{1}{2} \overline{\dim}_B X(\omega) = \frac{1}{2} \overline{\dim}_B \overline{X}(\omega) \geq \begin{cases} 1/4, & \text{if } \ell = 2, \\ 1/2, & \text{if } \ell \geq 3, \lambda = 1, \\ 1/(2\lambda + 2), & \text{if } \ell \geq 3, \lambda > 1. \end{cases}$$

Therefore,  $\dim_H E \geq c$ , where  $c$  is given as in (1.1). It contradicts the assumption that  $\dim_H E < c$ . This completes the proof of Theorem 1.2 in Case (i).

*Case (ii):* the sequence  $(|MP_1^j v|)_{j=0}^\infty$  is not constant.

For any integer  $p \geq s_1$ , let  $n = n_p$  be the largest integer so that  $s_n \leq p$ , and define

$$(3.16) \quad u_{1,p} = \rho_{i_1 \dots i_n}^{-1} \gamma_1^p Q_n P_1^{p-s_n} v, \quad u_{2,p} = \rho_{i_1 \dots i_n}^{-1} \gamma_1^{p+1} Q_n P_1^{p+1-s_n} v;$$

taking  $k = p - s_n$  and  $p - s_n + 1$  in (3.12) respectively, we have

$$(3.17) \quad u_{1,p}, u_{2,p} \in E - E.$$

By (3.16), we have

$$(3.18) \quad \frac{|u_{2,p}|}{\gamma_1 |u_{1,p}|} = \frac{|MP_1^{p+1} v|}{|MP_1^p v|} \quad \text{for all } p \geq s_1.$$

Furthermore, by (3.9)-(3.10), there exist two positive constants  $c_1, c_2$  so that

$$(3.19) \quad |u_{1,p}|, |u_{2,p}| \in [c_1, c_2] \quad \text{for all } p \geq s_1.$$

Now let  $W$  denote the closure of  $\{P_1^p : p \geq 0\}$  in  $\mathcal{O}(d)$ . As we have assumed,  $W$  is a connected subgroup of  $\mathcal{O}(d)$ .

Write

$$U^* = \{|x_1 - x_2| : x_1, x_2 \in E\} \cap [c_1, c_2].$$

Define

$$\pi_1 : U^* \times U^* \rightarrow \mathbb{R}, (u_1, u_2) \mapsto \frac{u_2}{\gamma_1 u_1}$$

and

$$\pi_2 : W \rightarrow \mathbb{R}, g \mapsto \frac{|MP_1 g v|}{|M g v|}.$$

It is clear that  $U^*$  is a compact subset of  $[c_1, c_2]$  with  $c_1 > 0$ , thus  $\pi_1$  is Lipschitz and  $\pi_1(U^* \times U^*)$  is compact. Moreover,  $\pi_2$  is continuous. By (3.17)-(3.19) and noting that  $W$  is also the closure of  $\{P_1^p : p \geq s_1\}$ , we have

$$(3.20) \quad \pi_2(W) \subset \pi_1(U^* \times U^*).$$

We claim that  $\pi_2$  is not a constant function. Otherwise, suppose that

$$\frac{|MP_1 g v|}{|M g v|} = a$$

for all  $g \in W$ . We have  $a \neq 1$  since the sequence  $(|MP_1^p v|)_{p=0}^\infty$  is not constant. If  $a < 1$ , then  $|MP_1^p v| \rightarrow 0$  as  $p \rightarrow \infty$ , and so  $|M g v| = 0$  for some  $g \in W$ . This is

impossible since  $M$  is invertible. If  $a > 1$ , then  $|MP_1^p v| \rightarrow \infty$  as  $p \rightarrow \infty$ . This is also impossible since  $|P_1^p v| = |v|$  for all  $p \geq 0$ .

Due to the above claim and the connectedness of  $W$ , the set  $\pi_2(W)$  is connected and contains at least two different elements, hence it is a non-degenerate interval. Therefore by (3.20),

$$4 \dim_H E \geq \dim_H U^* \times U^* \geq \dim_H \pi_1(U^* \times U^*) \geq \dim_H \pi_2(W) = 1.$$

Thus,  $\dim_H E \geq 1/4 \geq c$ , a contradiction again. Therefore Case (ii) can not occur. This completes the proof of Theorem 1.2.  $\square$

#### 4. FINAL QUESTIONS

Here we pose several questions about Theorem 1.5:

- (Q1) The lower bounds given in Theorem 1.5 on the lower box-counting dimension of  $(\alpha_1, \dots, \alpha_\ell)$ -orbits might not be sharp. Are there any better or optimal bounds? How about the packing dimension of the closure of these sets? <sup>2</sup>
- (Q2) It is easy to see that Theorem 1.5 can be extended to high dimensional tori. Is it possible to extend the result to general compact Lie groups?

**Acknowledgements.** The authors are grateful to Wen Huang for helpful discussions and to Pablo Shmerkin for pointing out the reference [16]. The first author was partially supported by the HKRGC GRF grants (projects CUHK401013, CUHK14302415). The second author was partially supported by NSFC (11471124 and 11371148).

#### REFERENCES

- [1] A. Algom, Embeddings of Cantor sets on the line. preprint, arXiv:1607.02849 [math.DS].
- [2] J. Deng, Z.-Y. Wen, Y. Xiong, and L.-F. Xi. Bilipschitz embedding of self-similar sets. *J. Anal. Math.*, 114:63–97, 2011.
- [3] Q.-R. Deng, and K.-S. Lau. On the equivalence of homogeneous iterated function systems. *Nonlinearity*, 26:2767–2775, 2013.
- [4] Q.-R. Deng, and K.-S. Lau. Structure of the class of iterated function systems that generate the same self-similar set. preprint, to appear in *J. Fractal Geom.*
- [5] M. Elekes, T. Keleti, and A. Máthé. Self-similar and self-affine sets: measure of the intersection of two copies. *Ergodic Theory Dynam. Systems*, 30(2):399–440, 2010.
- [6] R. Engelking. Sur un problème de K. Urbanik concernant les ensembles linéaires. *Colloq. Math.*, 8:243–250, 1961.
- [7] K. J. Falconer, *Fractal geometry. Mathematical foundations and applications*. Wiley, 2003.
- [8] K. J. Falconer, and D. T. Marsh. On the Lipschitz equivalence of Cantor sets. *Mathematika*, 39(2):223–233, 1992.
- [9] D.-J. Feng, W. Huang, and H. Rao. Affine embeddings and intersections of Cantor sets. *J. Math. Pures Appl. (9)*, 102(6):1062–1079, 2014.

---

<sup>2</sup>In Theorem 1.5(i), since  $\dim_H(K - K) = 1$ , by [20, Theorem 3] we have  $\dim_P K \geq 1/2$ .

- [10] D.-J. Feng, H. Rao, and Y. Wang. Self-similar subsets of the Cantor set. *Adv. Math.*, 281:857–885, 2015.
- [11] D.-J. Feng, and Y. Wang. On the structures of generating iterated function systems of Cantor sets. *Adv. Math.*, 222:1964–1981, 2009.
- [12] H. Furstenberg. Intersections of Cantor sets and transversality of semigroups. In *Problems in analysis (Sympos. Salomon Bochner, Princeton Univ., Princeton, N.J., 1969)*, pages 41–59. Princeton Univ. Press, Princeton, N.J., 1970.
- [13] M. Hochman. Geometric rigidity of  $\times m$  invariant measures. *J. Eur. Math. Soc.*, 14(5):1539–1563, 2012.
- [14] M. Hochman, and P. Shmerkin. Equidistribution from fractal measures. *Invent. Math.*, 202(1):427–479, 2015.
- [15] J. E. Hutchinson. Fractals and self-similarity. *Indiana Univ. Math. J.*, 30(5):713–747, 1981.
- [16] Y. Katznelson. On  $\alpha\beta$ -sets. *Israel J. Math.*, 33(1):1–4, 1979.
- [17] P. Mattila. *Geometry of Sets and Measures in Euclidean Spaces*. Cambridge University Press, 1995.
- [18] J. F. Price. *Lie groups and compact groups*. London Mathematical Society Lecture Note Series, No. 25. Cambridge University Press, 1977.
- [19] P. Shmerkin. On Furstenbergs intersection conjecture, self-similar measures, and the  $L^q$  norms of convolutions. Preprint.
- [20] C. Tricot. Two definitions of fractional dimension. *Math. Proc. Cambridge Philos. Soc.*, 91(1):57–74, 1982.
- [21] M. Wu. In preparation.

(De-Jun Feng) DEPARTMENT OF MATHEMATICS, THE CHINESE UNIVERSITY OF HONG KONG, SHATIN, HONG KONG

*E-mail address:* djfeng@math.cuhk.edu.hk

(Ying Xiong) DEPARTMENT OF MATHEMATICS, SOUTH CHINA UNIVERSITY OF TECHNOLOGY, GUANGZHOU, 510641, P. R. CHINA

*E-mail address:* xiongyng@gmail.com